Department of
INFORMATION
TECHNOLOGY

Maryland Data Security Policy

Last Updated: 06/08/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology is committed to managing the confidentiality, integrity, and availability of information processed, stored, or transmitted by its information technology (IT) networks, systems, and applications (IT Systems). Protecting the confidentiality of the information entrusted to the State of Maryland by its residents is vitally important to maintaining that trust. Effective data classification is paramount to protecting and controlling access to information, which allows the State to ensure confidential data is only accessed by those personnel whose duties require it.

The Maryland Department of Information Technology (DoIT) will utilize the definitions and guidelines relating to Public and Confidential Information established by the State of Maryland and relevant laws, such as 2013 Maryland Code §§10-1301 – 1308 to classify and protect its information. Access and security controls will be derived from standards and processes established by NIST Special Publication (SP) 800-53R4, SP 800-60 Vol I & Vol II, SP 800-111, SP 800-114R1, and NISTIR 7316: Assessment of Access Control Systems.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 3.1: Information Classification Policy and Section 7: Technical Level Controls and any related policies declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
06/08/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all Executive Branch agencies collecting, processing, storing, and transmitting any confidential information, including electronic content and physical media such as paper, discs, and memory storage devices. Ensuring confidential data is accessed only by agency staff with a **need-to-know** and implementing proper security controls to prevent unauthorized access will mitigate the risk of a data breach.

All agencies are responsible for protecting their information and enforcing this policy and any related policies. Employees, contractors, and vendors of IT resources and anyone else handling confidential data are also responsible for adhering to this policy.

4.0 Policy

This policy establishes the requirements for the Maryland Department of Information Technology and Executive Branch agencies to provide **due care** and **due diligence** in protecting and handling confidential data. The following subsections describe the agencies' responsibilities for data classification and for managing security controls to prevent unauthorized access (and dissemination).

4.1 Data Classification

For more information on data classification, refer to the *DoIT Public and Confidential Information Policy*. All Maryland State information is categorized into two main classifications regarding disclosure:

- Public Information
- Confidential (Non-Public) Information, which includes:
    - Personally Identifiable Information (PII)
    - Privileged Information
    - Sensitive Information

Due to the unique mission and business function of each agency, agencies are considered the owners of their own data, and are therefore responsible for classifying and managing their own data. Each agency understands the value of the information it collects, creates, and processes, so data owners must assess and label their data appropriately. Proper classification allows IT administrators and information security personnel to create effective system policies, processes, and technologies to restrict users from accessing data inappropriately; security controls will follow a need-to-know model while facilitating security capabilities to identify and track confidential information across the network.

Data owners must identify clear guidelines for tracking access-requests from both internal and external users; ensure all requests are properly documented and approved; and ensure access is promptly revoked per policy and operational criteria, such as when an employee is terminated or transferred (see *DoIT Account Management Policy*).

Once a data classification scheme is enforced and security controls have been implemented to protect against unauthorized access, agencies must also ensure that storage solutions protect data appropriately.

Additionally, data has a known tendency to be “migrated” to more places than owners are aware of. Therefore, periodic (data) scanning is required; automated tools can detect data-in-transit and determine if data is leaving an agency’s network without authorization, such as being sent to the Internet or being transferred to another media.

4.1.1 Data Retention

Agencies are required to develop a Retention Schedule (as directed in MD State Government Code Ann. § 10-609) that defines and documents **confidential data** retention requirements within the agency. Certain regulations, such as IRS 1075, dictate specific time frames and must be identified within the agency data inventory and retention directives, while other regulations, like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), only make retention recommendations; each agency must explicitly define how long data will be stored and archived.

Agencies will review their data inventory annually and archive or purge expired data. This will help prevent the costs associated with storage and backups from becoming excessive while minimizing the risks attributed to data compromise or breach. Agency backups will adhere to each agency retention schedule and will be reviewed at least annually for expired data.

4.1.2 Data Storage

Two primary concerns exist when protecting data storage: physical protections (e.g., offsite storage or cabinets with locks for backup media) and logical protections (e.g., encryption and access control [see section 4.2]).

Physical Protections

Due to the threat of confidential data compromise, storage and backup solutions must provide the physical protections listed in the table below. Note that logical protections — such as generating log events when the datacenter is accessed after hours — can be layered on top of physical controls to provide more comprehensive security solutions.

#	Storage Medium	Protection Requirement
A	Server Storage	Install locked faceplates on servers.
B	Rack Doors	Lock equipment racks containing servers or networking devices.
C	Datacenter Access	Lock access doors, and preferably use badging access-control to track users entering datacenter.
D	Backup Tape Drives	Configure with passwords to prevent unauthorized users from removing tapes from backup systems or tape libraries.
E	Local Backup Storage Cabinets	▪ Ensure blank backup tapes or other media ready for use are stored separately from media that already contain (backup) data ▪ Lock cabinets containing current backups to prevent unauthorized users from “borrowing” media already containing backup data
F	Offsite Storage	▪ Lock offsite storage facilities, and preferably track access by badged entry ▪ Lock all storage cabinets
G	Disaster Recovery Plan	Plan for controlling access to and collecting and transporting backup media to the disaster recovery site.
H	Periodic Audit	Take an annual inventory of backup media; inventory should be conducted by the asset manager, backup administrator, and the Information System Security Manager (ISSM), or delegate, to ensure all media are accounted for and that physical protections remain effective.

4.1.3 Data Loss Prevention

Once data has been classified, or labeled according to its information type, and security controls are in place, tools should be used, as feasible, to discover data-at-rest in inappropriate locations, such as project files stored on a local system instead of in a shared, secured location.

Periodic data discovery can help detect and determine whether confidential data is being stored in systems that may not have the required security controls, thereby putting information at higher risk of compromise.

If data has been properly classified, data loss prevention tools can also scan systems and media with data storage capabilities (e.g., network attached storage arrays (NAS), local hard drives, and USB flash memory drives) for specified parameters such as keywords, regular expressions, and meta data tags. Some tools can provide automated analysis for more comprehensive tracking and discovery.

Data loss prevention (DLP) is the process and capability of discovering data-in-transit and locating data-at-rest, discovering and tracking the movement of information, and blocking the export of information from a network. For more information regarding media transfers (i.e., USB flash drives, CD/DVD, etc.) refer to the *DoIT Media Protection Policy*.

Agencies utilizing DLP solutions must have qualified personnel properly configure and maintain the tools to ensure normal business functions are minimally affected. DLP administrators will ensure any false positive results are reviewed for legitimacy and any potential security events will be reported to the ISSM immediately. Agencies utilizing cloud storage solutions should preferably choose FedRAMP-compliant cloud service providers and ensure that data uploaded to the cloud can be tracked and discovered (for more information on cloud solution policies and security requirements, see *DOIT Cloud Services Security Policy*).

4.2 Access Control

Access controls are logical data protections that can be implemented through embedded software or through third-party products. These logical protections include: enforcing security controls across the domain or within network devices, logging and alerting on specific activities (using an aggregating analysis tool), and establishing permission groups to control access to restricted content.

Security controls will be implemented based on data categorization (Low, Moderate, and High values, as directed by FIPS-199) and will abide by policy and regulatory requirements. Access controls will be implemented in such a way that users will be restricted from accessing data not pertinent to their roles or assigned duties. Access controls help prevent large amounts of data from being stolen, in the event of an account compromise. The controls also help protect against insider threats and reduce the scope of compromise by a malicious user.

Physical access controls (e.g., badge readers) will be implemented to restrict users to spaces relevant to their work — for instance, users in the finance department should not have access to IT spaces and electrical closets. This will minimize the exposure of data and systems to unauthorized users as well as track access attempts to unauthorized spaces.

Piggybacking, or tailgating, to secured spaces is unauthorized and is considered a policy violation (see *DoIT Physical and Environmental Protection Policy*)

4.2.1 Network Segmentation

Network administrators can create virtual local area networks (VLANs) for network switches and routers; this is a form of micro-segmentation used to separate the network into smaller units with the effect of controlling for both data-at-rest and data-in-transit. These micro segmentations can be based on physical or logical groups like geography (e.g., all second-floor workstations) or function (e.g., Contracts and Finance Department) or may even be customized based on the agency's specific requirements. With a network divided into logical segments, systems can be prevented from communicating directly to systems in "outside" segments, therefore any compromised host or malicious traffic has a limited scope of compromise and less impact on operations.

Network administrators must ensure that only hosts that require access to the confidential information residing in a VLAN are members of that VLAN; the VLAN may be further segmented (e.g., segmenting PII for HR use and creating another segment for budget or tax data for the Finance department).

4.2.2 Technical Security Policies

A trusted group of clients and servers that share resources and operate under centralized security management is called a "domain". A domain can be set up to incorporate a variety of security controls that prevent users and clients from accessing resources and data not required by their job functions, while ensuring access is authorized for users who do need it. Windows Group Policy is an example of a tool used to manage security controls in a domain.

Technical security "policies" will be defined for user, networking, and security controls at the device level. IT administrators and information security engineers will ensure these technical security policies are configured to establish the security controls identified in NIST SP800-53R4 and SP800-53A, to meet the requirements set forth in DoIT's Cybersecurity Program and supporting policies, and to incorporate security industry best practices for logging the widest range of events and providing maximum visibility of network and system events.

4.2.3 Account Management

Users (including administrators) must authenticate to the network to be granted access to the data, applications, and services required to perform their jobs. In order to authenticate, users must have valid accounts on the domain. Accounts must be configured with security controls to enforce **least privilege**, ensuring minimum levels of access. Users will have access only to the information and resources required to do their jobs and will need to formally request additional access. Ensuring least privilege significantly protects against data theft by limiting what information is accessible to an adversary should a user's account be compromised, such as through a weak password or a user leaving a workstation unlocked. For more information, see *DoIT Account Management Policy*.

4.2.4 Group Memberships and Permissions

Group membership typically determines what data and resources a user has access to. Administrators and information security engineers will establish logical (access) groups for core business and mission units, and work with those units to determine the granular requirements for group access to shared stores, services, software, and even remote and system accesses; groups should be configured to enforce least privilege, and can also be used to establish access controls that can be monitored for indications of compromise.

Data owners and creators may also restrict access to specific data, files, or folders based on confidentiality and need-to-know. Data owners may establish groups (permission sets) to authorize user access, and also to ensure that system accounts, such as the backup service account, maintain minimum access for the service functionality. Data may be periodically reviewed to determine correct membership and permission attributes as well as to ensure that data is protected at the level required for its classification.

4.2.5 Remote Access

The *DoIT Remote Access Policy* describes more specifically the requirements for remote access. Data security is paramount when external connections, such as VPNs or remote desktops, are accessing critical resources from potentially untrusted systems or networks, thus exposing agency data to compromise or theft. Restricting remote access to only those users who require it allows those accounts to be monitored closely to prevent unauthorized use and to protect against data breaches.

External connections will be closely monitored by the Security Operations Center for unauthorized account access and indicators of compromised data-in-transit.

4.2.6 Mobile Device Access

The *DoIT Mobile Device Security Policy* describes more fully the requirements to control mobile device usage within the network. Accessing data through mobile devices is a primary data security concern. Administrators and information security engineers need to implement DLP solutions that control and track confidential information accessed and transmitted to mobile devices. Mobile Device Management (MDM) solutions must ensure that data remains protected at the level of classification required through policy or regulation while preventing data from being exposed to untrusted devices. Confidential information stored or handled on mobile devices is at serious risk of loss or theft. The devices themselves are exposed to threats and compromise when connecting to untrusted networks, such as coffee shop or airport WiFi.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The *Cybersecurity Program Policy* mandates this policy. Additional related policies include:

- Account Management Policy
- Cloud Services Security Policy
- Continuous Monitoring Policy
- Media Protection Policy

- Mobile Device Security Policy
- Public and Confidential Information Policy
- Remote Access Policy

7.0 Definitions

Term	Definition
Confidential Data	Confidential information is non-public information that, if disclosed, could result in a negative impact to the State of Maryland, its employees, or citizens and includes the following sub-categories: ▪ Personally Identifiable Information; ▪ Privileged Information; and ▪ Sensitive Information For more information on confidential information see *DoIT Public and Confidential Information Policy*.
Due Care	Using reasonable care to protect the interests of an organization. Developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures that are implemented through an organization's infrastructure.
Due Diligence	Practicing the activities that maintain the due care effort. The continued investigation and application of security into the existing infrastructure of an organization.
Least Privilege	The security objective of granting users only those accesses they need to perform their official duties.
Need-to-know	Security principle that confidential information will only be given to people who need it to do a particular job.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for creating and enforcing policies for agencies under its policy authority. The Enterprise and all Executive Branch agencies must exercise due diligence and due care to secure data by enforcing data security controls and least-access privileges to users to protect all State data.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize DoIT to shutdown external and internal network connectivity until such time the agency becomes compliant.

Any personnel responsible for the deliberate or inadvertent disclosure of confidential information may, pending the results of an investigation, be held liable and subject to disciplinary action, which may include written reprimand, suspension, termination, and possibly criminal and/or civil penalties.